УДК 004.8:327.88
DOI: https://doi.org/10.22182/spm.7112021.9
Прегледни рад

Српска политичка мисао
број 1/2021.
год. 28. vol. 71
стр. 201-221

Марија Ђорић*

Институт за политичке студије, Београд

Тања Милошевић**

Факултет политичких наука, Београд

ЗЛОУПОТРЕБА ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ У ЕКСТРЕМИСТИЧКЕ И ТЕРОРИСТИЧКЕ СВРХЕ***

Сажетак

У раду се истражује могућа злоупотреба вештачке интелигенције у екстремистичке и терористичке сврхе. Имајући у виду све већу дигитализацију и роботизацију друштва, сасвим је реално очекивати и све већу употребу вештачке интелигенције у безбедносном контексту, што ће свакако злоупотребити екстремистичке и терористичке групе. Аутори описују кроз низ релевантних примера на које све начине терористи злоупотребљавају вештачку интелигенцију, стављајући посебан акценат на употребу беспилотних летелица, тј. дронова. У раду се најпре елаборирају савремени трендови у одређењу феномена екстремизма и тероризма, проналазе се њихове тачке додира и дистанцирања, да би се у наставку детаљно анализирала употреба дронова у деловању тзв. „Исламске државе", „Хезболаха" и Хута у Јемену. Циљ рада је процена опасности коју екстремисти и терористи представљају по савремено друштво, у контексту злоупотребе вештачке интелигенције.

Кључне речи: беспилотне летелице, дронови, вештачка интелигенција, тероризам, екстремизам, насилни екстремизам, „Исламска држава", терористичка организација, безбедност

* Имејл-адреса: mara.djoric@yahoo.com.

** Имејл-адреса: tanja.z.milosevic@gmail.com.

*** Рад је настао у оквиру научноистраживачке делатности Института за политичке студије, коју финансира Министарство просвете, науке и технолошког развоја Републике Србије.

УВОД

Савремени свет је пред многобројним безбедносним изазовима, а један од највећих је свакако и екстремизам. Аморфност екстремизма, његова вишеслојност и комплексност, у великој мери утичу на неразумевање овог феномена, па самим тим и отежавају његову превенцију. Имајући у виду да живимо у дигиталној ери у којој се комуникација све више одвија у „онлајн простору", не можемо а да се не запитамо какве ће све то компликације имати по светску безбедност, посебно када је реч о екстремистичким активностима.

Волтер Лакер (*Walter Laqueur*) поставља два суштинска питања која се тичу будућности тероризма и екстремизма (Laqueur and Wall 2018):

1. Зашто се ове негативне појаве догађају?
2. Када ће то престати?

На прво питање, он даје наизглед неочекиван одговор, тврдећи да су национализам и демократија утрли пут насиљу екстремиста и терориста, док је друго питање и даље обавијено велом тајни (Видети: Đorić 2018). Чини се да је проблем савременог друштва у томе што се све више бави последицама, а не стварним узроцима екстремизма и тероризма. Поистовећивање ових наизглед сличних, а поново различитих феномена је још један у низу како практичних, тако и академских изазова. Осим тога, политизација тероризма и екстремизма и двоструког етичких стандарда умногоме отежавају њихово спречавање.

Футуристичко гледање на тероризам је неизвесно, управо због тога што је реч о глобалној појави од које више нико није „пелцован". Предиктивне дугорочне прогнозе о терористичким нападима је тешко направити, имајући у виду да се тероризам попут камелеона прилагођава новонасталим околностима. Многе светске силе су развиле одређене софтвере за препознавање лица, праћење кретања терориста, пресретање комуникације, и сл. Међутим, треба имати на уму да дигитализација друштва подједнако иде на руку и терористима и екстремистима који врло перфидно користе савремена научна и техничка достигнућа за реализацију својих идеолошких циљева. „Сајбер-тероризам" или злоупотреба интернета у терористичке и екстремистичке сврхе је присутна

више но икада.[1] Пропаганда коју екстремисти користе широм света за регрутацију нових чланова се тешко може зауставити, упркос труду друштвених мрежа да заједничким акцијама цензуришу њихово деловање.[2] Злоупотреба интернета се не одвија само на нивоу пропаганде, већ постоји и опасност да се уз помоћ рачунарских мрежа изврши напад на критичну инфраструктуру једне земље. Замислимо само шта би било када би терористи одлучили да уз помоћ вештачке интелигенције продру у систем комуникација авиосаобраћаја, нуклеарних електрана, водоснабдевања...?

Да би се предвиделе терористичке активности, неретко се користи систем *SNA* (*Social Network Analysis*), на основу којег су направљене потенцијалне математичке формуле за предикцију тероризма (Fujita et al. 2020). На први поглед ово звучи иновативно и корисно, али, заборавља се једна веома битна ствар, а то је да су феномени попут тероризма и екстремизма подложни друштвеној динамици, која је често непредвидљива и условљена сијасетом фактора.

Тако је, на пример, пандемија вируса *COVID-19*, која се јавила 2020. године, направила велики заокрет ка информатици, „онлајн" комуникацији и убрзаној дигитализацији друштва. Наше реално се трансформисало у „наше виртуелно", а вештачка интелигенција више није изузетак, већ постаје саставни део нашег живота. Промене у „новој нормалности" су такве да ће, уместо људског фактора, све више бити употребљаване машине, са посебним фокусом на вештачку интелигенцију. Оваква роботизација друштва ће имати значајне консеквенце и на безбедност, а посебно ће бити интересантно на које ће све то начине вештачка интелигенција[3] бити злоупотребљена за потребе екстремиста и терориста.

1 Ова два израза се у литератури често поистовећују, док постоје и они истраживачи који праве јасну дистинкцију међу њима. Такође треба напоменути да се „сајбер-тероризам" погрешно поистовећује са „сајбер-криминалом". Иако су ови појмови међусобно повезани, не можемо их сматрати идентичним. Више о томе видети у: NATO 2015.

2 Схвативши колика опасност прети од екстремистичке и терористичке пропаганде, Фејсбук, Мајкрософт, Твитер и Јутјуб су 2017. године направили „Глобални интернет форум за борбу против тероризма" (*Global Internet Forum to Counter Terrorism – CIFCT*). Циљ овог форума је била цензура терористичких садржаја и умрежавање стручњака, како би се створили контра-наративи. Према: Đorić 2020.

3 У наставку ће се користити скраћеница - ВИ.

САВРЕМЕНО СХВАТАЊЕ ФЕНОМЕНА ЕКСТРЕМИЗМА И ТЕРОРИЗМА

Једна од најчешћих грешака, како у академским, тако и у практичним истраживањима, јесте стављање знака једнакости између тероризма и екстремизма. Ова два (само) наизглед иста појма, међусобно се преплићу на више нивоа, стварајући забуну код читалачке публике. Екстремизам и тероризам се разликују у многим аспектима, посебно када је реч о законским регулативама.[4] Разликују се и по времену настанка, па тако тероризам (у феноменолошком контексту) бива етаблиран тек у 19. веку, захваљујући деловању руских анархиста.[5] Тачно временско етаблирање екстремизма у стручној литератури је тешко одредити, али се засигурно може рећи да је екстремизам 80-их година 20. века постао саставни део академског дискурса (Đorić 2020a). Да ли то значи да ове појаве нису постојале пре наведених временских одредница? Одговор је негативан, посебно када је реч о екстремизму који се, уколико узмемо у обзир његову етимологију, може сматрати понашањем (или мишљењем) на граници дозвољеног, са тенденцијом да се пређе наведена граница (Đorić 2014). Овим долазимо до закључка да екстремно понашање одвајкада постоји у људској природи, с тим што се екстремизам као друштвени (и пре свега политички) феномен етаблирао много касније.

Суштински гледано, екстремизам је много шири (еластичнији) феномен од тероризма и оставља више простора за манипулацију.[6] Тероризам је увек – потврђени екстремизам на делу, што би упрошћено значило да екстремиста може имати насилне идеје, претити, користити говор мржње, али кад почне да дела – онда се све више приближава тероризму. То би значило да је сваки тероризам у исто време и екстремизам, али не и *vice versa*. Да би екстремизам дошао до нивоа тероризма, потребно је да има политички мотив,

4 На пример, у Кривичном законику Републике Србије је тероризам одређен као кривично дело, док са друге стране, не постоји кривично дело екстремизма, иако се могу срести његови синоними попут говора мржње, дискриминације, изазивања националне, расне и верске мржње и нетрпељивости, и сл.

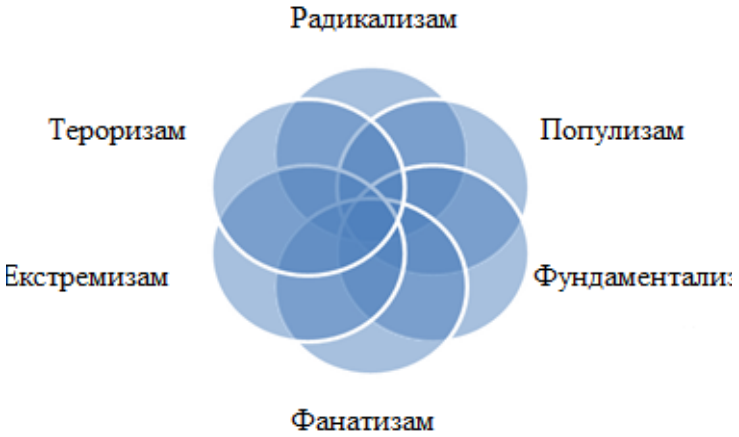
5 Добар пример је руска анархистичка организација „Народна воља", која је организовала атентат на руског цара Александра II.

6 Управо због тога се данас реч „екстремиста" или „екстремизам" све више користи за дисквалификацију политичких противника, без обзира на то да ли је то истина.

политички циљ, и у крајњем – политичке последице. Отуда је и једна од главних разлика између тероризма и екстремизма – политичност. Док је тероризам политички појам *par excellence*, екстремизам се не мора нужно јавити само у сфери политике, па тако издвајамо екстремизам у спорту, култури, религији... Као тачка амалгамирања између тероризма и екстремизма се налази тзв. насилни екстремизам (*Violent Extremism*). Реч је о феномену који се употребљава од недавно, те је термин „борба против насилног екстремизма" (*Counter Violent Extremism – CVE*), званично усвојен тек 2015. године на председничком самиту САД (*U.S. Presidential Summit*) (Neumann 2017). Осим насилног, постоји и тзв. „ненасилни екстремизам" (*Non Violent Extremism – NVE*), који је најпрецизније још 2014. године објаснио Алекс Шмид (Schmid 2014). Сагледавање екстремизма се додатно компликује уколико се истраживање усмери ка његовој класификацији, јер се могу пронаћи различите врсте, у зависности од критеријума који се употребљава.

Да би се разумела повезаност између екстремизма и тероризма, али у исто време уочила и дистинкција међу њима, направили смо графички приказ, уз помоћ којег се јасно очитава на који начин се ови појмови преплићу (укључујући и друге сродне феномене попут радикализма, фанатизма и тд.).

Слика бр. 1



Извор: Đorić 2020.

Ма колико на први поглед екстремизам деловао безазленије у односу на тероризам, он није за потцењивање, јер је сваки тероризам најпре морао да крене од екстремистичког система вредности. Управо због тога је и свака мудра борба против тероризма усмерена на превенцију екстремизма.

Када је реч о екстремистичким и терористичким трендовима, они се смењују по етапама. Тако је, на пример, током 70-их и 80-их година 20. века светом доминирао левичарски тероризам, да би почетком 21. века на сцену ступио „исламистички" фундиран тероризам, који се у последње време све више перципира као „џихадистички тероризам".[7] „Крешендо" џихадистичког тероризма је свакако био напад 11. септембра, док се по бруталности највише истакла тзв. „Исламска држава". Како свака акција изазива реакцију, тако је и овај тероризам добио одговор у виду десничарског екстремизма и тероризма. Мигрантска криза и криза изазвана пандемијом вируса *COVID-19* ће само интензивирати ксенофобију, екстремни национализам и страх за егзистенцију, што ће само отворити врата екстремној десници, а то ће бити свакако нова фаза у развоју савременог тероризма.

У том контексту ће од посебног значаја бити праћење активности екстремиста и терориста који ће у будућности своју пажњу највероватније усредсредити на два кључна сегмента:

1. Могућност злоупотребе вируса ради уцене политичких противника (биотероризам);
2. Све активније коришћење вештачке интелигенције зарад реализације политичких циљева.

ПОЈАМ ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ (ВИ)

Идејни творац појма „вештачка интелигенција", Џон Мекарти (*John McCarthy*)[8], дефинисао је 1956. године ову

7 Чак и у погледу семантичког одређења тероризма се јављају велике конфузије. Тако је у почетку деловање терористичких група попут „Ал Каиде", „Исламске државе", „Боко Харама" (и њима сличних), називано најпре „исламским", касније „исламистичким тероризмом", да би данас Европол у својим класификацијама користио израз „џихадистички" тероризам. Поједини теоретичари избегавају чак овај префикс (исламски/исламистички) како се не би угрозила верска осећања припадника исламске вероисповести који су умерени верници и који немају никаквих додирних тачака са екстремистима и терористима који спроводе идеологизацију религије.

8 Амерички научник који је 1971. године добио Тјурингову награду за допринос на пољу вештачке интелигенције.

област у сфери рачунарских наука као „науку о инжењерингу и изградњи интелигентних машина" (Boden 2018). Педесет година касније, област проучавања вештачке интелигенције још увек свакодневно бележи нове успехе и нова достигнућа, али је циљ остао исти. За потребе овог рада, користићемо свеобухватнију дефиницију ВИ коју је предложио Савет за истраживање инжењерских и физичких наука, а која гласи: „технологије вештачке интелигенције имају за циљ репродуковање или превазилажење (у компутативним системима) способности које захтевају „интелигенцију" уколико би [те процесе] изводили људи. То укључује: учење и прилагођавање, сензорно разумевање и интеракцију; резоновање и планирање; оптимизацију процеса и параметара; аутономију; креативност; и екстраховање знања и предвиђања из велике и разноврсне [количине] дигиталних података" (McKendrick 2019).

Директор одсека за анализу података компаније *Science Soft* Алекс Бекер (*Alex Bekker*) пружа врло једноставну типологију ВИ, делећи је на пет категорија: 1) интерактивна ВИ (пример: лични асистенти попут *Siri, Cortana* и *Alexa*); 2) функционална ВИ (роботи); 3) аналитичка ВИ (анализа података, *machine learning*); 4) текстуална ВИ (препознавање текста, конверзија говора у текстуалну форму); 5) визуелна ВИ (технологија проширене стварности) (Bekker 2019). Међутим, и информатичари и инжењери и аналитичари се слажу да, у савремено доба, ниједан истраживач не делује само у окриљу једног од наведених поља, већ своја истраживања и производе базира на интердисциплинарном приступу наведеним типовима ВИ.

Од појаве личних асистената попут софтвера *Amazon Alexa, Cortana* и *Siri* на глобалном тржишту 2011. године (када се појавио софтвер *Siri*), забележено је неколико случајева хаковања наведених софтвера, при чему је дошло до крађе личних података корисника. Иако наведени софтвери делују наизглед у потпуности бенигно, те се не сматра да могу представљати опасност по физичку безбедност корисника, истраживачи из Кине и САД указали су 2018. године на могућност упућивања скривених порука софтверима *Siri*, *Alexa* и *Google's Assistant*, којима се директно издају наредбе за приступање телефону. Узевши у обзир постојање технологије

IoT[9] и повезивање не само кредитних картица, већ и кућних уређаја са датим софтверима, таквим поступањем отвара се могућност да хакери не само пребаце новац са рачуна, већ и искључају улазна врата стана, или упале шпорет, примера ради. Група студената са Универзитета у Калифорнији је 2016. године спровела експеримент са наведеним софтверима кроз усађивање скривених порука у песме доступне на *YouTube* платформи, а које нису препознатљиве људском уху, и тиме навеле дате софтвере да приступе паметним уређајима у кући (Smith 2018). Иако до сада није забележен такав случај, експерименти попут наведеног указују на могућност спровођења напада кроз хаковање софтвера, при чему би такав софтвер могао, примера ради, изазвати експлозију или пожар, са потенцијалним смртним исходом.

Са друге стране, концепт *machine learning*, то јест, машинског учења, даје врло значајан допринос борби против радикализације и детекције потенцијалних терориста, при чему је допринос највидљивији у оквиру процеса истраживања података (eng. *data mining*) – откривања шаблона у великим скуповима података коришћењем машинског учења, статистичке анализе и анализе базе података. Овај процес се може вршити на најосновнијем нивоу, попут анализе дискурса терористичких и екстремистичких организација кроз анализу објава званичних портпарола или лидера наведених групација[10], до анализе велике количине материјала (у текстуалној, аудио или видео форми) употребом статистичке анализе и софтвера за проналажење репетитивних секвенци, које могу чак довести до ране детекције пропагандних материјала на интернету, али и до откривања потенцијалних терориста и спречавања терористичких напада. Таквим активностима се углавном баве државне институције[11] и

9 Сам појам „Интернет ствари" (eng. *Internet of Things, IoT*) односи се на међуумрежавање физичких предмета, уређаја, зграда и других ствари које у себи садрже било који вид електронике, софтвера или чипа, са другим објектима, тачније, рачунарима, преко интернета, што им омогућава размену података. Више о томе у: Hilts et al. 2019.

10 На пример, Ел Нашар и Најеф (2019) пружају опсежну анализу 17 званичних саопштења тзв. „Исламске државе" у периоду од 2014. до 2016. године у свом раду: Nashar and Nayef 2019. Међутим, аутори напомињу да у анализу нису укључили фотографије приложене уз материјале, као ни пропагандни материјал те организације, којим би, процесом истраживања података кроз машинско учење, пропагандни материјал лакше, брже и ефективније анализиран, а такође би такав вид анализе обухватио и већу количину материјала.

11 Америчка Национална сигурносна агенција (*National Security Agency*) је 2007. године у Пакистану користила алгоритам *SKYNET* за анализу метаподатака прикупљених са 55 милиона мобилних телефона локалних корисника, те је вршила класификацију

безбедносни органи, али у последње време и међународне и невладине организације и мултинационалне компаније.

Најзначајнији корак по питању превенције радикализације и ширења пропагандних материјала екстремистичких група направила је друштвена мрежа *Facebook*, која од 2017. године користи концепт машинског учења ради ефективнијег уклањања непримереног садржаја, при чему су такву праксу данас усвојиле и друге платформе као што су *Microsoft, Twitter, Google, Amazon* и *YouTube*.[12] Наредни изазов који стоји пред друштвеним мрежама јесте превенција пропагирања радикалних и екстремистичких идеја уживо, на шта је указао напад на џамију и исламски центар у Крајстчерчу на Новом Зеланду 15. марта 2019. године, када је терориста објавио пренос напада уживо.[13]

Узевши у обзир да је текстуална вештачка интелигенција инкорпорирана у концепт машинског учења, важно је напоменути да се, по питању анализе текста, ВИ може користити за анализу садржаја без асистенције људског фактора, док се софтвер за препознавање лица, као представник пете, визуелне категорије ВИ, може користити за детекцију присуства лица која су претходно идентификована као потенцијални терористи или екстремисти.

УПОТРЕБА ДРОНОВА У ЕКСТРЕМИСТИЧКЕ И ТЕРОРИСТИЧКЕ СВРХЕ

Последња типологија вештачке интелигенције у низу – функционална ВИ, уједно је и главна тема овог рада, а њен главни представник јесу дронови, то јест, беспилотне[14] и беспосадне летелице и пловила. Најједноставније речено, Николас Гросман (*Nicolas Grossman*), стручњак за неконвенционално

корисника у две групе: 1) лица која су се понашала као потенцијални терористи; и 2) остатак корисника. Више о томе у: McKendrick 2019.

12 Током прва три месеца 2019. године, *Facebook* је уклонио 2.2 милијарде лажних профила, а 65% објава које представљају говор мржње је одмах уклоњено. До септембра 2019. године, *Facebook* је уклонио више од 200 профила неонацистичких организација, а употребом ВИ и људске експертизе, уклоњени су садржаји и профили лица која пропагирају идеје тих група. Више о томе у: Wagner 2019. и Moltzau 2019.

13 Главни истраживач за ВИ друштвене мреже *Facebook* Јан Лекун (Yann LeCun) наводи да је анализа *live* садржаја и даље у току, али да главни проблем представља мањак материјала тог типа, те је стога врло тешко саставити алгоритме који ће тренирати препознавање насиља. Више о томе у: Vincent 2019.

14 У наставку рада – БЛ.

ратовање, дронове дефинише као „летеће роботе" (Grossman 2018). Међутим, и сам аутор касније, поред стандардних општепознатих модела беспилотних летелица, представља концепт *копнених дронова*, али и беспосадних пловила.

Речник *Merriam-Webster* пружа три дефиниције речи *дрон*: 1) мушка пчела без бодље која не прикупља нектар или полен - трут; 2) паразит; биће које живи од рада других (аналогија на пчелу која не учествује у прикупљању полена и нектара); и 3) беспосадна летелица или брод навођен даљинским управљањем или посредством уграђених рачунара (Merriam-Webster 2020). Сама етимологија речи указује на порекло дронова – наиме, од првобитне идеје да изграде човеколиког робота, научници су се током времена усмерили на изградњу робота по угледу на инсекте, углавном пчеле и мраве, тачније, оне које карактерише прилагодљиво понашање и социјализација (Boden 2018). Стога је врло јасно због чега поједине БЛ, као што је, на пример, модел *The Black Hornet Nano* норвешке производње, личе на инсекте.

Дронови су од експерименталних модела за спровођење мисија извиђања[15] ступили на историјску позорницу као оружје 04. фебруара 2002. године, када је *Predator*, навођен руком припадника Централне обавештајне агенције (*CIA*) извео први ваздухопловни напад у Хосту у Авганистану, са циљем елиминације Осаме бин Ладена (Sifton 2012). Од тог тренутка, БЛ су као оружје и метод елиминације непријатеља присутне у већини конфликата.

Четири године касније, 2006. године, „Хезболах" ће постати прва екстремистичка група која ће извести ваздухопловни напад на непријатељске положаје, у овом случају – на израелске мете, употребом БЛ. Наиме, према наводима израелских и иранских медија, ова шиитска група је од Ирана добила БЛ *Ababil* 2002. године, које је углавном користила за спровођење оперативних мисија прикупљања података на територији Израела, а које је 2006. године опремила експлозивним материјалом, а затим намерно сударила са метама од стратешког значаја за Израел. Међутим, први ваздухопловни напад који је „Хезболах" спровео без

15 Прва употреба БЛ америчке војске забележена је у Босни 1995. године, када је мали сквадрон БЛ *Predator* коришћен за спровођење извиђачких операција на терену. Наводи се да је до краја 1996. године изведено преко 1.575 мисија у ваздушном простору Босне. Више о томе видети у: Michel 2013.

жртвовања БЛ, који ће у историји бити запамћен као први ваздухопловни напад изведен употребом БЛ од стране једне екстремистичке организације, догодио се у септембру 2014. године, када су БЛ Хезболаха бомбардовале штаб Ал Нусра Фронта на сиријско-либанској граници (Gross 2016).

Наредни случај конфликта у којем је забележено активно коришћење БЛ у ратовању јесте текући грађански рат у Јемену, који је од 2015. године кулминирао у војну интервенцију суседних земаља окупљених под кишобраном Саудијске коалиције.[16]

Прва беспилотна летелица која је пролетела кроз ваздушни простор Јемена била је америчке производње, а у тој земљи се нашла са циљем елиминације истакнутог припадника Ал Каиде, Каеда Салима Сине ал Харитија[17], 2002. године. Петнаест година касније, 26. фебруара 2017. године, Хути су приказали четири БЛ, за које су тврдили да су их сами дизајнирали и саставили. Међутим, аналитичари ангажовани у сфери наменске индустрије указали су на чињеницу да БЛ именована *Qasef-1* умногоме подсећа на тип иранске БЛ *Ababil-II*[18], чије је постојање претходно забележено у редовима Хезболаха у Либану. Они су тврдили да, не само да дизајн БЛ Хуту подсећа на иранске БЛ, већ је и префикс серијског броја идентичан[19], што указује на два сценарија: 1) могући трансфер знања између Ирана и Хута; или 2) извоз иранских БЛ у Јемен за потребе побуњеничке

16 У грађанском рату у Јемену учествују три фракције: Међународно призната Влада Јемена, побуњеничка група Хута и снаге Јужног транзиционог савета. Поред локалних актера, девет арапских земаља окупљених у Саудијској коалицији (такође позната и као Арапска коалиција) – Саудијска Арабија, УАЕ, Судан, Бахреин, Кувајт, Катар, Египат, Јордан и Мароко, ангажују припаднике својих оружаних снага и снага безбедности на терену, при чему су три државе – Судан (2019), Катар (2017) и Мароко (2019), до сада окончале своје ангажовање у Јемену.

17 Ал Харити је сумњичен да је учествовао у извођењу терористичког напада на *USS Cole* у октобру 2000. године, као и у нападу на танкер *Limburg* током пловидбе Аденским заливом у октобру 2002. године.

18 Наведени тип БЛ производи иранска компанија *Aircraft Manufacturing Industrial Company – HESA*.

19 Узастопни бројеви након идентичних префикса такође указују на чињеницу да су наведене БЛ произведене у истој серији и на истом месту, а детаљном анализом компонената (мотора и жироскопа), аутори студије су утврдили да су оне идентичне онима које се користе у производњи иранских дронова. У питању су двоцилиндрични мотор *DLE 111* кинеске истоимене компаније и жироскоп *Model V10*. Према процени јеменског истраживачког центра *Abaad Studies & Research Center*, цена мотора износи око 600 УСД, док је цена пропелера који се користи у изградњи ових БЛ, а који они идентификују као производ немачке компаније *Benchwood*, износи око 250 УСД. Оба производа се могу купити преко интернета.

борбе, уз негирање извоза пропагирањем приче о „домаћој производњи" (Conflict Armament Research 2017). Поред наведеног модела *Qasef-1*, Хути наводе да су произвели и друге моделе летелица – *Al Hudhud, Al Hudhud-1, Al Raqib, Sumad 2, Sumad 3,* и *Qasef-2M*, наглашавајући да они те БЛ користе не само за спровођење напада на Саудијску коалицију и поименице Саудијску Арабију, већ за прикупљање података и надгледање терена и противничких снага. Наиме, они су своју „флоту БЛ" поделили на: 1) дронове за прикупљање података[20] и 2) дронове за извођење самоубилачких мисија.[21] Међутим, дронови за извођење самоубилачких мисија свакако носе много веће последице, чему иде у прилог чињеница да су Хути, извођењем ваздухопловног напада на постројење Абкаик, као и на нафтно поље Хураис и пратеће постројење за прераду нафте, оба у власништву саудијске компаније *Aramco*, 14. септембра 2019. године привремено зауставили производњу нафте, која се претходно кретала у обиму око 5,7 милиона барела дневно, што чини око 5% глобалног ланца снабдевања нафтом. Као последица напада, компанија је била приморана да користи залихе нафте како би испунила обавезе по питању извоза, као и да експлоатише нафту из морских бушотина. На глобалном нивоу, напад на нафтна постројења довео је до скока цене нафте са 54.80 УСД на 62.67 УСД по барелу (пораст од 14%) (Greenley 2019).

Случај употребе технологије у редовима Хута значајан је помена из још једног разлога: наиме, 19. септембра 2019. године, само пет дана након извођења напада на постројења компаније *Aramco*, та побуњеничка група је покушала да

20 Хути користе четири типа БЛ за извиђање – *Hudhud, Hudhud 1, Raqib* и *Rased. Hudhud* је дужине 150 цм и ширине 190 цм, а може изводити налет у трајању до 90 минута у рејону од 30 км; *Raqib* је дужине 100 цм, распона крила 140 цм, и може изводити налет у трајању од 90 минута у рејону од 15 км; *Rased* је дужине 100 цм и ширине 220 цм, и може изводити налет у трајању од 120 минута у рејону од 35 км. Наведени дронови су углавном сличних конституција, с тим што је *Raqib* такође опремљен термовизијским камерама. Истраживачи наводе да су наведене БЛ врло сличне иранским БЛ *Tlash 1* и *Muhajir 1*, које је Иран користио током рата са Ираком осамдесетих година 20. века.

21 У питању су БЛ модела *Qasef-1, Sumad 2, Sumad 3, Qasef-K2.* Чланови јеменског истраживачког центра *Abaad Studies & Research Center* наводе да детаљан опис ових БЛ није познат широј јавности, али да Хути наводе да модели *Sumad 2* и *Sumad 3* могу да изводе налете у трајању од 24 часа у рејону од 1.000 км. С друге стране, модел *Qasef-1* има рејон од 150 км и долет носивости до 30 км, дужине је 250 цм и распона крила од 300 цм; може да изводи налете у трајању од 120 минута. Истраживачи наведеног института наводе да Хути ове БЛ наоружавају углавном експлозивима, те да Хути често не планирају да исту БЛ користе два пута, већ само једном. Више о томе видети у: Abaad Studies & Research Center 2019.

спроведе напад на пловила саудијске морнарице на Црвеном мору употребом беспилотних пловила, у којима је једини терет био - експлозив.[22] Идентични инциденти забележени су и са бродовима који у територијалним водама Јемена плове под заставом УАЕ, као и са стратешки значајним лукама у територијалним водама Саудијске Арабије.

Последњи значајан пример у низу односи се на активности тзв. „Исламске државе", која је врло озбиљно пригрлила погодности које са собом носи употреба беспилотних летелица у асиметричном ратовању. Балкан у својој публикацији из 2017. године наводи да су ирачке снаге безбедности регистровале употребу БЛ од стране тзв. „Исламске државе" још 2015. године, те да је та организација користила БЛ за „шпијунирање непријатеља и прикупљање информација" (Balkan 2017), али и за извођење ваздухопловних напада на непријатељске положаје. Први ваздухопловни напад изведен БЛ регистрован је 27. септембра 2016. године, када је БЛ испустила експлозивни материјал на припаднике оружаних снага Турске у Сирији, након чега је уследио и први напад на територији Ирака 02. октобра исте године, сада на положаје курдских Пешмерга (Lock 2019). За разлику од Хезболаха и Хута, тзв. „Исламска држава" се није снабдевала дроновима од Ирана, већ документи откривени у Ираку указују на то да је та организација планирала, а донекле и спровела, куповину, унапређење и развијање технологије у сфери беспилотних летелица (Rassler 2017), и то вероватно на црном тржишту. Документ откривен у једном од упоришта тзв. „Исламске државе" у Ираку открио је информације о шест мисија које ће изводити наведене БЛ, а које су се углавном заснивале на шпијунирању, извођењу ваздухопловних напада и тренажним летовима. Поред тога, податак да је тзв. „Исламска држава" своје дронове опремала *GoPro* камерама указује на врло значајан аспекат употребе БЛ – снимање напада и пропагандних материјала (Al Arabiya 2017). Узевши у обзир да су у питању дронови које је тзв. „Исламска држава" купила или сама унапредила, важно је напоменути да је та организација углавном прибављала квадкоптере вредности између 650 и 1.000 УСД, који имају

22 Први напад овог типа забележен је 30. јануара 2017. године, када су беспосадна пловила Хута, натоварена експлозивом, ударила у саудијску фрегату *Al Madina* у близини лучног града Ходејда у територијалним водама Јемена. Више о томе видети у: Lock 2019.

могућност извођења налета од 10 до 30 минута, и којима се може управљати са удаљености до седам километара, те се главни значај употребе БЛ у том контексту заснива на опреми – професионалним камерама. Од највећег значаја за анализу употребе технологије у редовима тзв. „Исламске државе" ради радикализације осетљивих група, а посебно омладине, јесте чињеница да, осим што су БЛ коришћене за снимање изведених напада, наведени снимци су често пре постављања на интернет едитовати тако да подсећају на компјутерске игрице (Balkan 2017).

И на нашим просторима су у више наврата коришћени дронови у циљу провоцирања, ширења говора мржње и стварања националне нетрпељивости. Један од најупечатљивијих примера јесте пуштање дрона са заставом „Велике Албаније" током фудбалске утакмице између Србије и Албаније, која је одржана 14. октобра 2014. године на стадиону „Маракана" у Београду. Дроном је управљао Албанац Исмаил Морина, који је ухапшен у Хрватској, по потерници Републике Србије (Blic 2020).

Наведена три случаја употребе беспилотних летелица од стране терористичких и побуњеничких група – Хезболаха, Хута и тзв. „Исламске државе", као и кратак опис примера злоупотребе БЛ на територији наше земље, пружају довољно материјала за извођење јасних закључака. Пре свега, важно је напоменути да, за сада, не постоји велики број терористичких организација и побуњеничких група које се користе овим технологијама за извођење напада. Куповина БЛ је још увек врло скупа инвестиција, те ни терористичке организације попут тзв. „Исламске државе", без „спонзорства" великих сила, не могу себи приуштити такву технологију. Међутим, као што је био случај са рачунарима, а затим и андроид телефонима, и БЛ ће постати све више и више присутне на комерцијалном тржишту, а самим тим и у терористичким и екстремистичким групама. Дронови представљају привлачно оруђе за извођење напада због чињенице да на тај начин терористичке групе избегавају жртвовање својих припадника и спровођење самоубилачких напада, чиме не умањују број својих припадника и симпатизера. Самим тим, очекује се да ће се у будућности такве групе све више и више окретати ка унапређењу постојећих технологија, као и прибављању јефтинијих модела БЛ за своје потребе.

Досадашње искуство нам указује на то да су, у случајевима када су забележени напади изведени БЛ, углавном у питању биле: 1) БЛ произведене од стране друге силе (и наведеним случајевима, Ирана); и 2) јефтинији модели БЛ доступни на интернету (комерцијални дронови) и БЛ домаће радиности, чије се компоненте могу лако набавити путем интернета. За сада се као највећи произвођач БЛ истиче кинеска компанија *DJI*, која се прославила производњом серије БЛ *Mavic*[23], и која тренутно производи око 70% комерцијалних БЛ доступних на глобалном тржишту, те се очекује да ће се модели те компаније, у нешто измењеном облику, у будућности налазити у рукама терориста и екстремиста. Узевши у обзир да нам случај тзв. „Исламске државе" указује на могућност употребе БЛ у пропагандне сврхе, важно је истаћи и америчку компанију *Ambrella*, која производи чипове за камере *GoPro* и дронове са уграђеним камерама, али и саму компанију *GoPro*, која је у сарадњи са компанијом *DJI* учествовала у дизајну и производњи БЛ у серији *Mavic* (Joshi 2019). Уз то, врло је важно пратити односе терористичких организација и великих светских сила, јер примери „Хезболаха" и Хута указују на могућност да „озбиљни играчи" на политичкој сцени, који имају јаке наменске индустрије, своје „донације" у будућности оплемене и БЛ.

Поред куповине комерцијалних БЛ, терористичке организације се могу ове технологије домоћи и хаковањем БЛ непријатељских снага. За сада, стручњаци наводе да је немогуће хаковати софистицираније БЛ, али је у неколико наврата забележено приземљивање БЛ непријатеља без наношења штете истом. Претпоставља се да је за приземљење дронова коришћена техника *spoofing*, при чему се изводи напад на *GPS* летелице тако да се она „збуњује" и „убеђује" да слети на друго место које хакер предодреди, а које ће БЛ третирати као своју базу, то јест, локацију која је претходно предодређена за слетање након окончања мисије. Томе у прилогу иде чињеница да се програмер Марк Сзабо (*Mark Szabo*) на конференцији о етичком хаковању 2016. године пред учесницима преузео контролу над БЛ *Parrot AR* (Grossman 2018).

23 БЛ овог произвођача се на интернету могу прибавити по цени од 500 до 1.500 УСД.

ЗАКЉУЧАК

Анализом наведена три случаја, ауторке су дошле до закључка да терористичке организације могу злоупотребљавати БЛ на неколико начина. Поред конвенционалног надгледања терена, прикупљања података о непријатељу и терену на којем ће се изводити напад, као и очекиваног спровођења терористичких напада, БЛ се могу користити и као средство за припрему пропагандног материјала којим ће се спроводити радикализација потенцијалних терориста. Највећу бригу, у том погледу, изазива чињеница да су ти материјали углавном намењени младима, узевши у обзир настојања да снимке напада, живота у терористичкој организацији, погубљења и других терористичких активности, аутори пропагандног материјала обрађују како би више подсећали на видео игре, популарне међу омладином.

Иако будућност тероризма делује застрашујуће, имајући у виду да се употребом ВИ повећава његов деструктивни потенцијал, чињеница је да ни безбедносне службе широм света неће седети „скрштених руку". Оно што можемо очекивати јесте да ће се рат између Добра и Зла у врло скоријој будућности све више водити у „сајбер" простору, уз употребу роботике, вештачке интелигенције и рачунарских система. Отуда је сасвим логично да државе усмере своје потенцијалне ресурсе у едукацију стручњака који ће бити способни да одговоре на све изазове које са собом носи данашња „нова реалност".

РЕФЕРЕНЦЕ

Abaad Studies & Research Center. 2019. *Suicide Drones... Houthi Strategic Weapon.* Special File: Strategy Unit. Last access: February 13, 2020. https://abaadstudies.org/pdf-37.pdf

Balkan, Serkan. 2017. *Daesh's Drone Strategy: Technology and Rise of Innovative Terrorism.* SETA – Foundation for Political, Economic and Social Research, Istanbul, Turkey.

Bekker, Alex. 2019. *5 Types of AI to Propel Your Business*. Poslednji pristup 29. avgust 2020. https://www.scnsoft.com/blog/artificial-intelligence-types

Boden, Margaret. 2018. *Artificial Intelligence: A Very Short Introduction.* Oxford: Oxford University Press.

Blic. 2017. "Albanac koji je pustio dron u Beogradu zatražio azil u Hrvatskoj." 28. avgust 2020. https://www.blic.rs/vesti/hronika/albanac-koji-je-pustio-dron-na-utakmici-u-beogradu-zatrazio-azil-u-hrvatskoj/lvpl4sf.

Conflict Armament Research. March 2017. *Iranian Technology Transfers to Yemen: 'Kamikaze' drones used by Houthi forces to attack Coalition missile defence systems.* Poslednji pristup13. februar 2020. https://www.conflictarm.com/wp-content/uploads/2017/03/Iranian-Technology Transfers-to-Yemen.pdf

Djoric, Marija. 2018. „On Violence and Nonviolence in Political Theory: Some Conceptual Dilemmas" *Serbian Political Thought* 18 (2): 127–140. doi.org/10.22182/spt.18212018.8.

Đorić, Marija. 2014. *Ekstremna desnica: međunarodni aspekti desničarskog ekstremizma*. Beograd: Nauka i društvo Srbije.

Đorić, Marija 2020. a *Nasilni ekstremizam: multidisciplinarni pristup.* Beograd: Institut za političke studije.

Đorić, Marija 2020. b *Priručnik za prepoznavanje, prevenciju i suzbijanje radikalizacije i nasilog ekstremizma kod učenika*. Podgorica: Biro za operativnu koordinaciju – Nacionalni operativni tim

El-Nashar, M and Nayef, H. 2019. *'Cooking the Meal of Terror'.*

Manipulative Strategies in Terrorist Discourse: A Critical Discourse Analysis of ISIS Statements. Terrorism and Political Violence.

Fujita, Hamido et. al. 2020. *Trends in Machine Learning Theory and Applications Machine Learning*, "A model for Predicting Terrorist Network Lethality and Cohesiveness", 33rd International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems, IEA/AIE 2020, Kitakyushu, Japan, September 22–25, 2020, Proceedings, Springer.

Greenley, Heather L. et al. 2019. *Attacks on Saudi Oil Facilities: Effects and Responses.* Congressional Research Service, Insight.

Gross, Judah Ari. Video appears to confirm use of attack drones by Hezbollah. 11 August 2016. https://www.timesofisrael.com/video-appears-to-confirm-use-of-attack-drones-by-hezbollah-in-syria/

Grossman, Nicholas. 2018. *Drones and Terrorism: Asymmetric Warfare and the Threat to Global Security.* I. B. Tauris, Bloomsbury

Hilt, S. et al. 2019. The Internet of Things in the Cybercrime Underground. https://documents.trendmicro.com/assets/white_papers/wp-the-internet-of-things-in-the-cybercrime-underground.pdf.

Laqueur Walter i Wall Christopher. 2018. *The future of terrorism: ISIS, Al-Qaeda, and the alt* right**.** New York: Thomas Dunne Books/St. Martin's Press.

Lock, James. 2019. *Saudi-Coalition Intercepts Houthi Unmanned Explosives-Laden Boats*. Maritime Security Review. https://www.marsecreview.com/2019/10/saudi-coalition-intercepts-houthi-unmanned-explosives-laden-boats/

McKendrick, Kathleen. 2019. *Artificial Intelligence Prediction and Counterterrorism*. Chatham House, The Royal Institute of International Affairs. Research Paper.

Michel, Arthur Holland. 2013. *Drones in Bosnia*. https://dronecenter.bard.edu/drones-in-bosnia/

Moltzau, Alex. 2019. *How Does Facebook define Terrorism in Relation to Artificial Intelligence?* https://towardsdatascience.com/artificial-intelligence-and-terrorism-in-social-media-cf166adaf78e;

Neumann, Peter. 2017. *Countering Violent Extremism and Radicalisation that Lead to Terrorism: Ideas, Recommendations, and Good Practices from the OSCE Region*, https://www.osce.org/chairmanship/346841?download=true.

Rassler, Don et al. 2017. *The Islamic State's Drone Documents: Management, Acquisitions and DIZ Tradecraft.* CTC Perspectives – West Point Combatting Terrorism Center.

Schmid, Alex. 2014. Violent and Non-Violent Extremism: Two Sides of the Same Coin?, https://www.icct.nl/download/file/ICCT-Schmid-Violent-Non-Violent-Extremism-May-2014.pdf.

Sifton, John. 2012. *A Brief History of Drones.* https://www.thenation.com/article/archive/brief-history-drones/.

Smith, Craig S. 2018. *Alexa and Siri Can Hear This hidden Command. You Can't.* https://www.nytimes.com/2018/05/10/technology/alexa-siri-hidden-command-audio-attacks.html.

NATO. 2015. *Terrorist use of cyberspace and cyber terrorism: new challenges and reponses*. Amsterdam**:** NATO, IOS Press.

Vincent, James. 2019. *Using AI to screen live video of terrorism is 'very far from being solved', says Facebook AI chief.* https://www.theverge.com/2019/5/20/18632260/facebook-ai-spot-terrorist-content-live-stream-far-from-solved-yann-lecun

Wagner, Kurt. 2019. *Facebook Removes a Record 2.2 Billion Fake Accounts.* https://www.bloomberg.com/news/articles/2019-05-23/facebook-removed-2-2-billion-fake-accounts-in-first-quarter

Marija Djoric*

Institute for Political Studies, Belgrade

Tanja Milosevic**

Faculty of Political Sciences, Belgrade

ABUSE OF ARTIFICIAL INTELLIGENCE FOR EXTREMIST AND TERRORIST PURPOSES

Resume

In this paper, the authors research possible abuse of artificial intelligence for extremist and terrorist purposes. Having the growing digitalization and robotization of the society in mind, it is completely realistic to be expecting a growing abuse of artificial intelligence in the security context, which will definitely be abused by extremist and terrorist groups. Artificial intelligence (AI) can be divided into five basic categories: 1) interactive AI (example: personal assistants such as *Siri, Cortana* and *Alexa*); 2) functional AI (robots); 3) analytical AI (data analysis, *machine learning*); 4) textual AI (text recognition, conversion of speech into textual form); 5) visual AI (augmented reality technology).

However, IT experts, engineers, and analysts all agree that, in the contemporary times, not a single researcher acts only within one of the previously mentioned fields, but conducts research and bases their products on an interdisciplinary approach to the said types of AI. Throughout a series of case studies, the authors analyse numerous ways in which terrorists might abuse artificial intelligence, with a special emphasis on the use of unmanned aerial vehicles, that is, drones. Drones have stepped out of the phase of experimental models for conducting reconnaissance missions and entered the historical stage as a weapon on February 04, 2002, when a *Predator*, piloted by the hand of a member of the Central Intelligence Agency (*CIA*) conducted the first airstrike in Khost in Afghanistan, with the goal of eliminating Usama bin Laden. Since that moment, UAVs are present as a method of eliminating the enemy in the majority of conflicts. In this paper are contemporary trends regarding the definition of extremism

* E-mail address: mara.djoric@yahoo.com.

** E-mail address: tanja.z.milosevic@gmail.com.

and terrorism elaborated, the points of contact and the points of distancing between them are determined, followed by a detailed analysis of examples of abuse of drones by terrorist organizations, such as the so-called "Islamic State" and "Hezbollah", as well as the Houthi rebel group in Yemen.

The main purpose of the paper is to estimate the danger extremists and terrorists pose to the contemporary society in the context of abuse of artificial intelligence. The conclusion is that, in the coming future, extremists will more and more use artificial intelligence for conducting their activities, including terrorist attacks.

Keywords: unmanned aerial vehicles, drones, artificial intelligence, terrorism, extremism, violent extremism, „Islamic State", terrorist organization, security

* Овај рад је примљен 24. јануара 2021. године, а прихваћен на састанку Редакције 23. фебруара 2021. године.